Workstation Security

HIPAA Security ◆ November 2003

TMA Privacy Office Information Paper

Records Management ◆ FOIA ◆ DUAs ◆ HIPAA Compliance ◆ ADP Security ◆ Privacy Act ◆ System of Records ◆ PIAs

Standard Requirement

Workstation security must be addressed as part of the physical safeguards of the covered entity. This standard requires implementation of "physical safeguards for all workstations that access electronic protected health information (EPHI), to restrict access to authorized users."

Workstation is defined as "an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment." (164.304) Thus PDAs, tablet computers, and other portable/wireless devices are included. DHHS noted specifically in its Final Rule commentary that the workstation standards are not to be interpreted as limited to "fixed location devices." (Final Rule, p.8340) The critical variable is not the particulars of the device itself, but whether it can access or store PHI. If it can, formal, documented policies and procedures must be in place, and the covered entity must take reasonable, appropriate steps to assure that the policies and procedures are followed.

This standard complements standard §164.310(b) by requiring covered entities to implement physical controls that grant workstation access to authorized users and prevent workstation access to unauthorized users. For fixed location devices, these might include specifications for secure locations. For portable ones, they might include limitations on what devices can leave the facility. The particular rules would be determined by, among other things, results from the covered entity's risk analysis and risk management efforts, required as part of the security management process standard. In its information security risk assessment, a covered entity should evaluate the threats and vulnerabilities of inappropriate physical access to workstations by unauthorized personnel. In its risk management plan, it should describe and justify the controls instituted to mitigate such threats and vulnerabilities. There are no associated implementation specifications with this standard.

See also:
45 CFR 164.310(c)
Device and media controls

Federal and DoD regulations that support this standard
DoD 8510.1-M
DoDI 8500.2